# PECAN+

BRISBANE, 3 AUG 2024

/WHOAMI

- Chief Evangelist & Principal OT Cyber Security Architect at Secolve

- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years

- Chartered Engineer (CPEng) and Registered Professional Engineer of Queensland (RPEQ)

- Chair of the Queensland Branch of the Information, Telecommunications and Electronics Engineering (ITEE) College

- Queensland President of the Australia Professional Engineers Association (APEA) and a proud member of Professionals Australia (PA) – The Union for STEM Workers

- Chair of the Queensland Branch of the Australian Information Security Association (AISA) and Lead of the AISA Security Architecture Special Interest Group (SecARCH SIG)

- Bach Eng (Telecomms) QUT and Master Business (Applied Finance) QUT

MY BACKGROUND

CYBER IS A BROAD DISCIPLINE
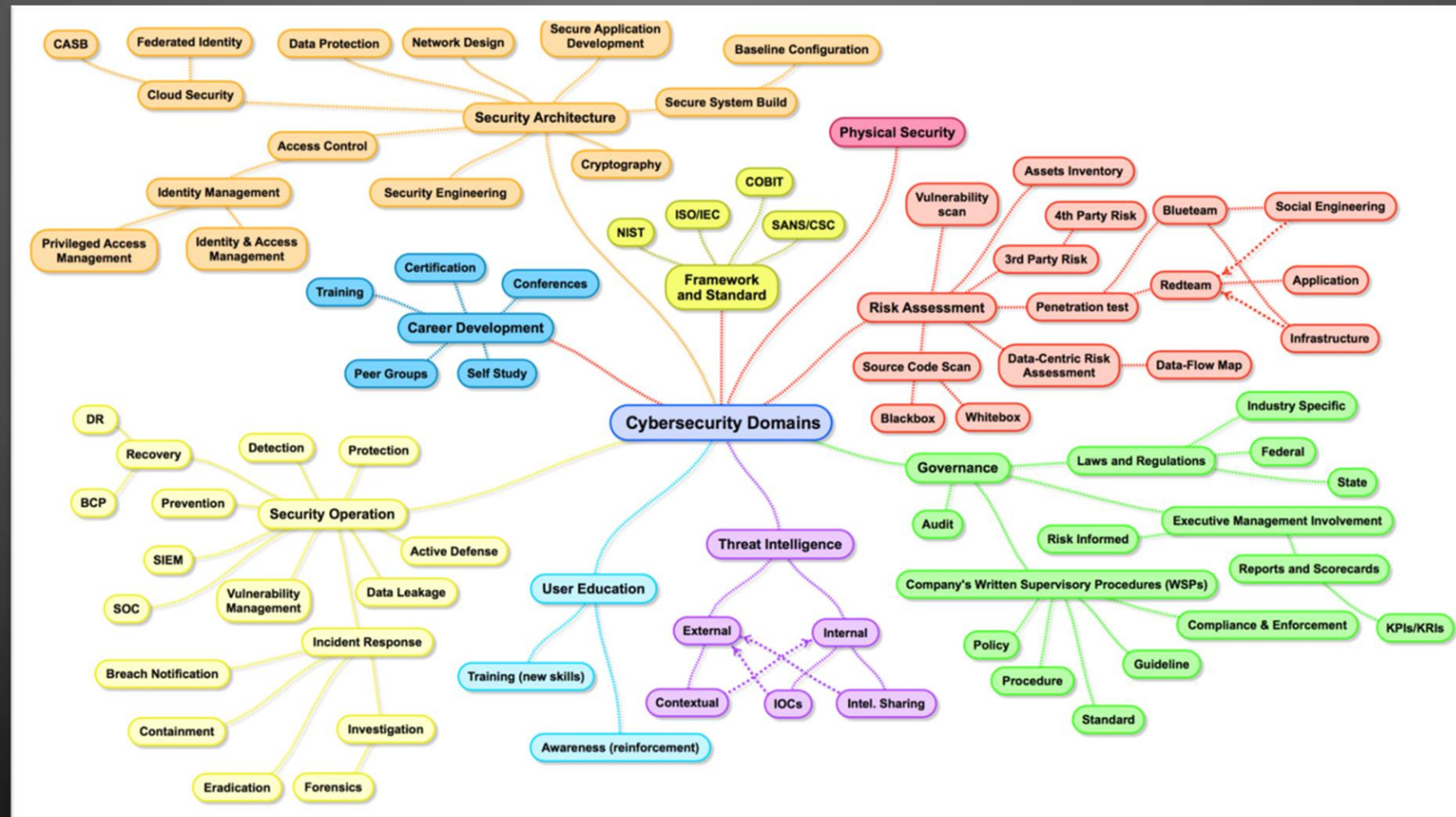
RED & BLUE, WHAT COLOUR ARE YOU?

QGCSU RESOURCES

Cyber security careers: Security operations

Find out about available roles, certifications and courses in the field of cyber security operations.

Cyber security careers: Governance, risk and compliance

Learn about available roles, certifications and courses in the field of cyber security governance, risk and compliance.

Cyber security careers: Security architecture

Find out about available roles, certifications and courses in the field of cyber security architecture.

Source - https://www.forgov.qld.gov.au/recruitment-performance-and-career/career-development/develop-digital-and-ict-capabilities/develop-your-cyber-security-skills

QGCSU RESOURCES CONT.

Cyber security careers: Security operations

This career stream provides leadership, analysis, monitoring and safeguarding system access and response and resolution to cyber security incidents within an organisation.

Speciality areas

- Customer service and technical support
- Incident and problem management
- Knowledge management
- Network security services
- Security Infrastructure System Administration
- Systems Security Analysis
- Incident Response
- Threat intelligence and cyber hunting

Example roles

- Manager Cyber Security Operations
- Lead Security Operations
- Lead Security Incident
- Lead Security Analyst
- Senior Security Specialist
- Security Specialist

Incident management

As defined by the SFIA foundation: Incident management is the processing and coordination of appropriate and timely responses to incident reports, including channelling requests for help to appropriate functions for resolution, monitoring resolution activity, and keeping clients appraised of progress towards service restoration.

Security administration
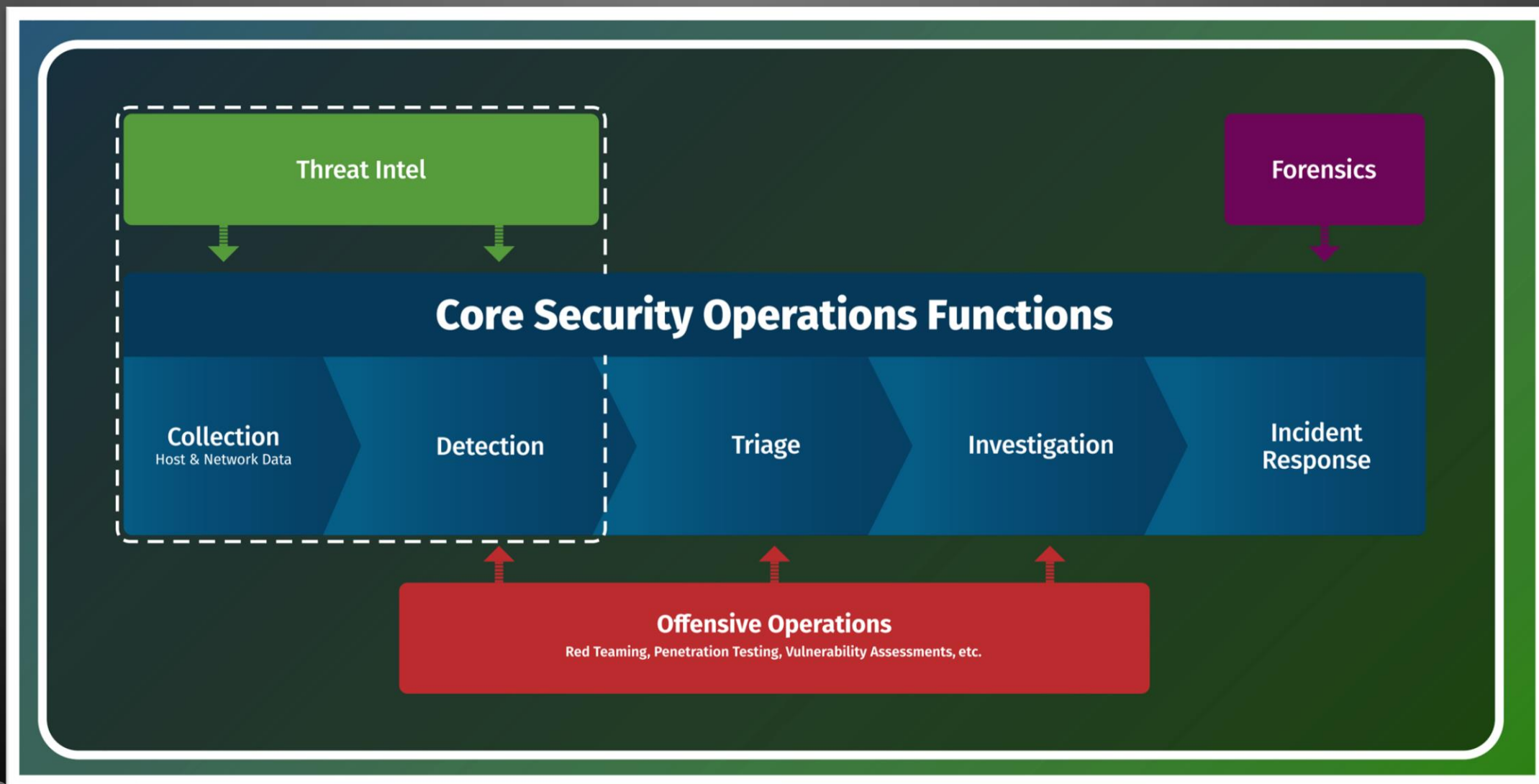
As defined by the SFIA foundation: Security administration is the provision of operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation.
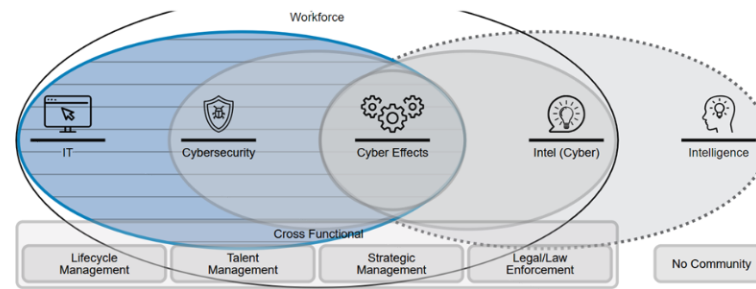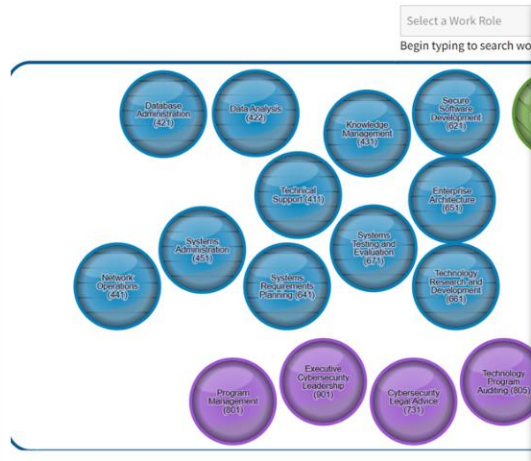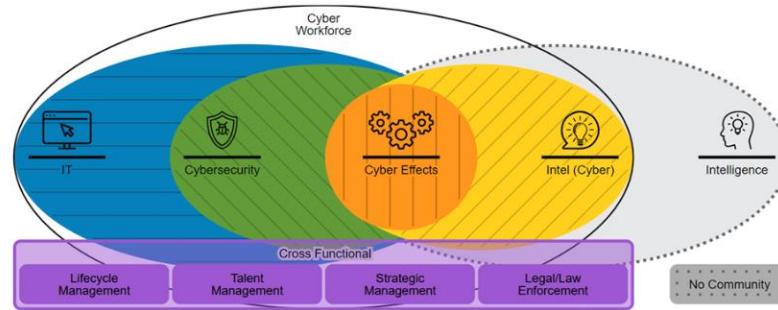
Digital forensics

As defined by the SFIA foundation: Digital forensics is the collection, processing, preserving, analysing, and presenting of computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

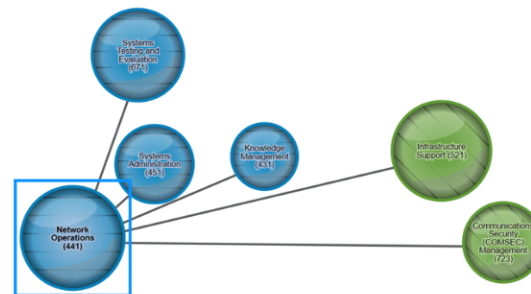Here are some ways you could build this skill, which applies to a range of cyber security roles.

SANS – GUIDE TO SOC OPERATIONS

NIST NICE

SOME TIPS ON WHAT TO DO

- **Remember, don't play on networks you don't own or have permission to be on!**

- Look at jobs that interest you and look at their skills and education requirements

- Make use of free online resources like LinkedIn Learning through State Library of Queensland, SANS on YouTube etc.

- There is a big difference between Formal Education, Certifications and Experience – think about what to do and when

- There are multiple ways in, sometimes you have to do something else to get experience to get into a cyber role

- Soft Skills Matter – <u>Learn how to communicate verbally and written</u>

- Go to Security Meetups – SecTalks, AISA, etc.

- Go to Security Conferences – BSides Brisbane, CrikeyCon, BrisSEC etc

THANK YOU, QUESTIONS?